Journal of Hardware and Systems Security (2017) 1:311–327
https://doi.org/10.1007/s41635-017-0028-8

TSensors Vision, Infrastructure and Security Challenges in Trillion Sensor Era

Current Trends and Future Directions

Mahabubul Alam[1] · Mark M. Tehranipoor[2] · Ujjwal Guin[1]

Received: 19 September 2017 / Accepted: 14 November 2017 / Published online: 28 November 2017

Abstract
With the advancement of ubiquitous computing under the hood of Internet of Things (IoT) and Cyber-Physical Systems (CPS), the number of connected devices is expected to grow exponentially in the following decade. Pervasive sensing is the backbone of any IoT/CPS application. Billions of connected devices each having multiple sensors will lead us to the age of trillion sensors. Widespread use of sensors in critical applications (e.g., smart grid, agricultural industry, food production, etc.) will present us with unique challenges. Identifying the threats well before they occur will be the key in the race against the threats posed by the adversaries in the age of trillion sensors (TSensors). In this paper, we present a detailed survey of the trends toward trillion sensors, and their applicability in recent connected applications. We identify several key areas, that need to be addressed to build a secure connected environment. There are several challenges and limitations as well which are expected to rise in the coming decade. We must be proactive in addressing those challenges to make a safe and secure environment.

Keywords Trillion sensors · Internet of things (IoT) · Supply chain · Physically unclonable functions (PUFs) · Encryption · Authentication

1 Introduction

1.1 Trillion Sensors (TSensors) Vision

The recent growth of IoT/CPS applications is leading us to the age of trillion sensors where trillions of sensors, which are spread geographically, will produce real time data for further analysis and decision making. Through real time data analytics, processes can be monitored for fault detection and diagnosis, control decisions can be made, excess resources in one area can be shared with another, and thus resource management can be optimized. Through proper resource sharing, global issues like shortage of sustainable energy, scarcity of clean water, lack of food, etc. can be combated effectively. Peter H. Diamandis et al. projected a need for 45 trillions networked sensors to solve many such global issues in just one generation (20 years) [31]. Environmental pollution monitoring, personal health monitoring, energy harvesting, food delivery, global disasters, and aging infrastructure monitoring—these are some of the business opportunities where trillions of sensors might be required. Smart sensing technologies enabled by embedded microprocessors and communication modules can be the key in such large-scale monitoring and control systems [81].

The introduction of smart phones revolutionized the sensor industry. In the period 2007–2014, the mobile sensor market experienced an exponential growth of nearly 200% which was not envisioned by any market research organization [24]. With virtual reality and internet of things expected to become ubiquitous in the coming decade, a

✉ Mahabubul Alam
mahabubul.alam@auburn.edu

Mark M. Tehranipoor
tehranipoor@ufl.edu

Ujjwal Guin
ujjwal.guin@auburn.edu

[1] Department of ECE, Auburn University, Auburn, AL, USA

[2] Department of ECE, University of Florida, Gainesville, FL, USA

similar growth is expected to sustain in the following decade as well. Historically, sensor development is a lengthy process. In spite of that, the global MEMS/NEMS industry was able to meet the demand for large volume of sensors in the smart-phone industry because the associated technology was already there and the types of sensors used in the smart-phone devices were limited. In this period, we have observed the rise of demand for microphones, acceleration sensors, magnetic sensors and gyroscopes from a mere 10 million units in 2007 to 10 billions in 2014 [25]. Modern smart-phone devices also adopted pressure, IR, humidity, temperature, light, and proximity sensors to support new applications. But, in the era of IoT and pervasive sensing, we will require large volume of application specific sensors which have to be developed in a tight schedule. Power consumption, accuracy, cost, and security will dominate the sensor development for different applications.

Currently, a typical smart-phone device uses around 15 sensors, a modern car uses approximately 200 sensors, a smart-home system uses around 100 sensors [25]. With the advancement in *mHealth* or *eHealth* technologies, number of wearable medical sensors (WMS) is on the rise. Presently, in the developed world, a person typically uses ten wearable sensors (basically WMS) [25]. For such day to day applications, cost will be the key factor for sensor development. Low-cost sensors will help these applications to spread more quickly among all market segments. The development of Industrial IoT (IIoT) by companies like GE to increase production efficiency, improve execution, and optimize their respective business through advanced real-time data analytics will increase the demand for sensors to monitor industrial processes and machines which will push the demand for application specific sensors further [13]. Following the aerospace industry, there is a trend in developing digital twins for expensive/critical industrial process/machines (like a digital twin for a power plant) which also requires large-scale real-time data collection and analysis and hence will increase the demand for various types of sensors [79]. In these industrial applications, accuracy of data is a key factor. In applications like $CeNSE$ of HP, where sensors will be placed in large geographical area, power consumption is a factor in choosing the right sensor technology [48].

According to Ericsson Mobility Report, 2016, IoT sensors and devices are going to takeover as the largest source of connected devices by 2018, growing at a 23% compound annual growth rate from 2015 to 2021 [69]. HP introduced Central Nervous System for the Earth ($CeNSE$) which is based on detectors and actuators, expected to reach trillion units by 2018 [48]. GE has shown a plan for 10 trillion pollution monitoring printed sensors for 2025 while Texas Instruments projected 13 trillions Internet connected devices by 2025 expecting sensors/MEMS to be the enabling technology [24]. Cisco delivered a forecast of 1 trillion networked sensors by 2020 whereas Bosch presented a vision of 7 trillions sensors by 2017 [24]. Intel introduced sensors for context aware computing and such systems are expected to absorb a trillions sensors by 2020-2022 [24]. Harbor Research considers smart systems to be the biggest business opportunity in the history of business which will fusion computing, communication, and sensing into one platform [10].

Figure 1 summarizes sensors forecast of different companies. Integrating large number of sensors in connected applications has its own challenges and limitations. Widespread use of sensors demands lower price for sensors which in turns results in low power budget, low die area allocation, low computational power, etc. Further, these sensors have to send the data to a server which raises the need for development of low resource communication technologies/protocols where security is often compromised. Designing such sensors under severe resource constraints is a challenging task which might raise piracy of such designs in the coming decade. Huge market demand can give rise to large scale sensor device counterfeiting through recycling, remarking, shipping rejected devices, and many other ways which have been affecting the global IC supply chain for a long time [85]. Embedding sensor nodes with

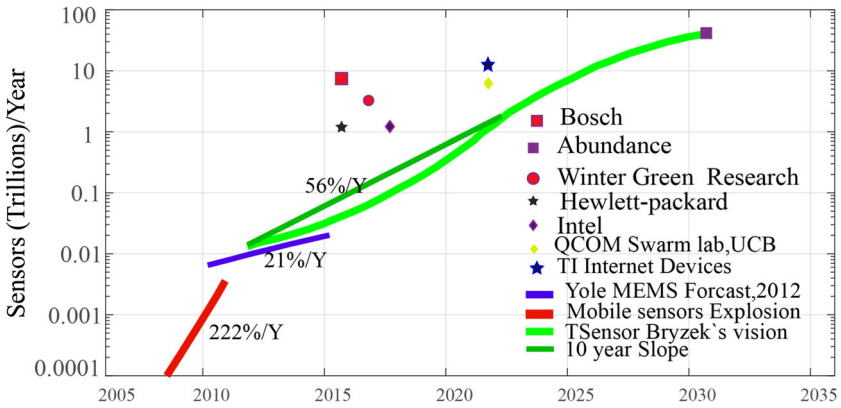

Fig. 1 Projected growth of sensors [24]

unique security primitives have been considered to secure the semiconductor supply chain.

The application domains of sensors are widely varied. Sensors used in different applications are selected based on different assessment parameters like price, power and performance. Identifying the sensors and sensor technologies used in different applications is necessary. Mobile devices and IoT/CPS applications are the biggest contributors of sensors. In a standard IoT/CPS architecture, the sensor node comes at the bottom of the framework connecting the physical world to the digital world and apart from sensing, the nodes must have some computing and communicating capabilities.

1.2 Contributions

The exponential growth in the global sensor market which had been brought by the smart mobile devices is expected to continue with the growth of virtual reality, IoT/CPS applications, and more. Diversity in sensor-based applications puts forward different application specific requirements for the sensor nodes in various connected systems. In order to support the exponential growth, the sensor nodes have to be low-cost and the resources have to be limited. The huge demand for sensors and complexities in designing resource constrained sensor nodes can attract large scale piracy, cloning, counterfeiting, as well as they can raise other security issues and privacy concerns. In this article, our main objectives are to present a vision of trillion sensors, identify the applications and architectures which might contribute the most number of sensors, asses their limitations and security vulnerabilities, provide a comprehensive discussions about the security threats, and finally focus on some preventive measures where substantial research work is necessary. To the best of our knowledge, this is the first article that incorporates all these topics. The main contributions of this article are as follows:

- *Taxonomy of Sensors:* In this paper, we have developed a comprehensive taxonomy of sensors based on their application domains, the technologies used for manufacturing, and their operating principles. Each category is populated with examples of sensors which have great potential to be used in large scale in variety of applications. The taxonomy will help us identify group of sensors used in different application domains.
- *Security Assessment:* Ensuring the security of a connected system poses difficult challenges, partly because there are such a wide variety of different sensors present in the component supply chain. It is of utmost importance to assess the vulnerability of a connected system that consists of hundreds of sensors. In this paper, we present different vulnerabilities originated from the resource limitations in low-end sensor nodes and identify the security threats that might arise both in the software and the hardware levels. We believe that this will help the researchers assess the limitations, devise security measures and protocols to counter these security issues, and provide a secure connected environment.
- *Research Directions:* We believe that research in designing a connected system that uses resource constrained sensor nodes in a connected environment is still in its infancy. There are several major challenges that must be overcome in the near future. In this paper, we provide a direction in ensuring security in sensor-based applications and identify areas where substantial research is necessary in order to secure the applications as well as the sensor supply chain. We believe, this will help the researchers channel their effort in the correct direction to build a secure connected system.

The rest of the paper is organized as follows. We present a comprehensive taxonomy of sensors based on application domains, technologies, and operating principles in Section 2. The infrastructure of sensor networks have been presented in Section 3. We present different challenges and limitations of sensor-based applications in Section 4. Section 5 focuses on the current development in the supply chain security research and low resource communications. We conclude our paper in Section 6.

2 Taxonomy of Sensors

Sensor-based applications can be classified into different application domains where each application domain will require domain specific sensors with varied area, power, and price constraints. These sensors can be further classified into different categories based on the technologies used to develop them. Sensors are developed by manipulating a particular physical property or a set of properties of some objects/materials. A sensor generally operates by converting energy from one form to another to detect any physical phenomena. The final form of energy is generally electrical. Sensor-based applications can be further classified based on their operating principles. In the following subsections, we present a taxonomy of trillion sensors based on applications, technologies, and operating principles of the sensors.

2.1 Applications

Sensors have found widespread usage in many applications. International Technology Roadmap for Semiconductors (ITRS) has identified sensor-based IoT applications to be the next driving factor for the semiconductor industry [18].

Companies like Libelium, GE, Intel, Cisco and AT&T have successfully implemented sensor-based industrial and domestic applications in the last few years [13, 17, 33]. TSensors movement has identified some market segments with large volume sensor use potentials [24]. Based on the initiatives taken by the major companies and the market segments identified by the TSensors movement, we have recognized seven major application domains where trillions of sensors are required (see Fig. 2). The application domains are discussed in the following section.

a) Mobile Computational Systems Mobile computational systems are a key market segment for MEMS. High-end mobile devices already boasts more than 15 sensors on average. Gyroscopes, accelerometers, GPS, touch, microphones, and proximity sensors are already commonplace in modern cell phones, tablets, PCs, and toys. Virtual reality devices are incorporating different types of motion sensors in order to recognize all types of messages that a human can convey through the motion of his limbs. To make our computing systems aware of the surroundings temperature, pressure, light, sound, and moisture sensors are finding their ways in modern computing devices.

b) Healthcare In the last few years, we have seen an explosion of wearable medical devices in the consumer market to facilitate healthcare. Free fall detection technologies have been built around accelerometer. Medical fridges have been built based on light, temperature, humidity, impact, and vibration sensors. Electrocardiography (ECG), pulse, and respiration sensors have paved the way for sportsmen care and patient surveillance devices. Ultraviolet (UV) sensors have enabled devices to produce radiation alert. Occlusion sensors are used in ambulatory infusion pumps, insulin pumps, and enteral feeding pumps to measure occlusions (blockages) in silicone or polyvinyl chloride (PVC) tubing.

c) Environmental Monitoring Environmental monitoring through geographically distributed sensors have assisted agriculture tremendously. Abbaco Controls, with help from Intel and Kontron, has deployed an IoT-based irrigation systems in Malaysia that allowed the farmers to control water supplies to their fields [1]. The system works based on real time data analytics on the data collected from large number of water level and temperature sensors distributed over the farming land. The system has almost doubled the rice production in Malaysia since its deployment. Cisco and Sprint have worked together to build a truly connected city in Kansas [2]. Light and video sensors deployed in the city have been used to develop smart lighting system and save significant amount of energy. There is huge potential in developing air quality monitoring and forest fire detection systems based on gas and temperature sensors.

d) Industrial Automation Sensors have played a crucial role in industrial automation for a very long time. Ubiquitous sensing and Big data analytics are opening new applications for industrial automation. Intel and Kontron have built a platform called Salesforce that monitor factory equipment's through the use of sensors and real-time data analytics,

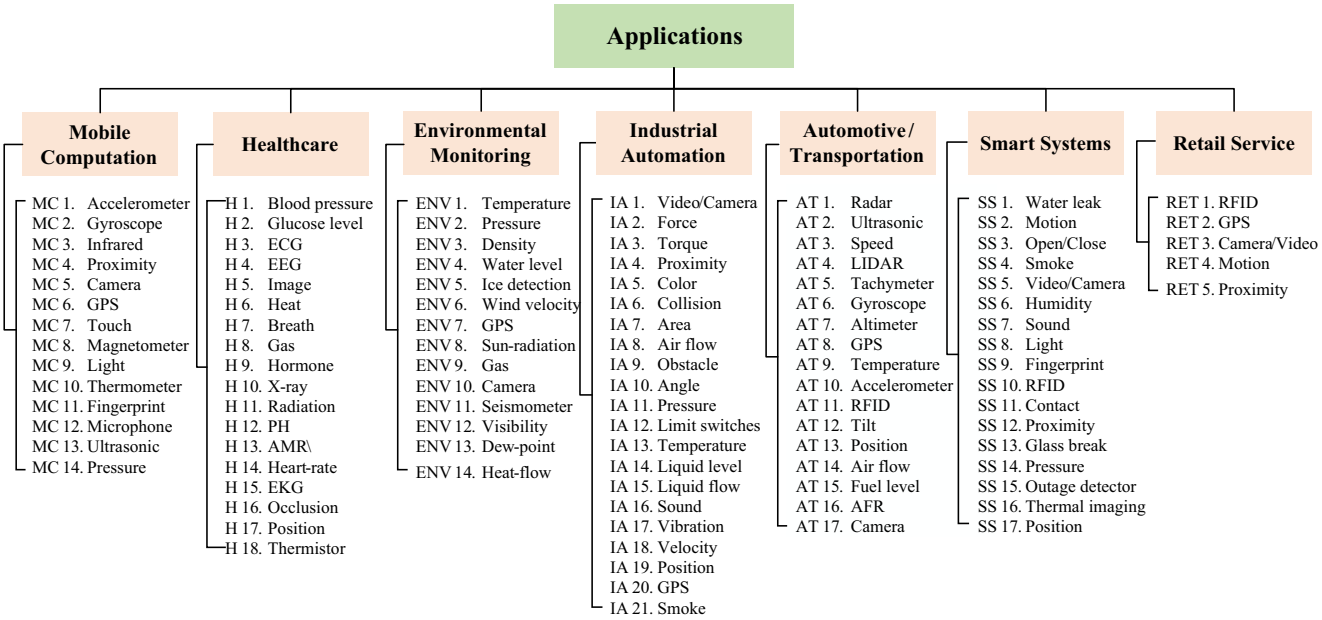

Fig. 2 Trillion sensors application domains

provides detailed error messages to the engineers, and quickly dispatches field service engineers to minimize unplanned factory downtime [3]. GE has identified location intelligence through GPS to be a key factor in factory automation [4]. Libelium has identified passive tags (RFID+NFC) and active tags (ZigBee, WiFi, Bluetooth) to be the enabling technologies for location intelligence [17]. Temperature, pressure, current, vibration, and gas sensors can bring new era of machine health monitoring systems which might increase the efficiency of manufacturing systems by a significant margin.

e) Automotive/Transportation Smart sensing and affordable communication technologies have paved the way for intelligent transportation. Video/Camera and proximity sensors with computer vision have enabled self-driving technologies. A modern vehicle incorporates around 30 sensors to facilitate safety features. Some cars and trucks are equipped with headway RADAR sensors that detect the distance between a vehicle and any vehicles or large objects in front of the vehicle. These sensors are used by adaptive cruise control and collision avoidance systems. Air flow meters are used to measure the air flow intake of automobile engines. LIDAR sensors are used in autonomous cars to provide 360° vision of the surroundings.

f) Smart Systems Smart systems integrate functions of sensing, actuation, and control in order to describe and analyze a situation. These systems make decisions based on the available data in a predictive or adaptive manner, thereby performing smart actions. Smart home is a prime example of smart systems. Water leak, smoke detector, glass break, light, sound, and fingerprint sensors are leading the way for smart home development. Leviton's smart home technology has been used to develop an independent living community for the seniors at Grand Rapids, Michigan where occupancy and humidity sensors are deployed to automatically turn exhaust fans [5]. They also provide an option to add free fall sensors to the system for elderly care.

g) Retail Service Smart retail service like Amazon Go, is using motion sensors and image sensors to automate their service [74]. RFID already playing a huge role in tracking deliveries for online stores like Walmart, postal deliveries and many other retail services [6]. Anti-theft devices are commonplace in retail stores which generally incorporate RFID tags for tracking particular products. The tags are deactivated upon purchase. If someone moves the product outside the store without deactivating the tag, it generates an alarm.

2.2 Operating Principles

Sensors are integral part of any electronic control applications. In an electronic system, a sensor provides a measurable electrical output (current/voltage) based on a physical phenomena through conversion of energy. Energy can be converted from chemical, mechanical, optical, thermal, etc. to electrical. The properties of materials that are manipulated to develop sensors can vary widely. We have identified seven major categories of sensors based on their operating principles (energy conversion topologies) which we believe will be essential in trillion sensors application development and the classification shown in Fig. 3.

a) Electrical/Electronic Electrical sensors examine the change in electrical or magnetic signals based on environmental input. Metal detectors, radar systems, voltmeters, and ohmmeters are few simple examples where electrical sensors are used. An application like a smart-grid or a smart-meter requires sensors that sense different electrical parameters like current, voltage, capacitance, resistance,

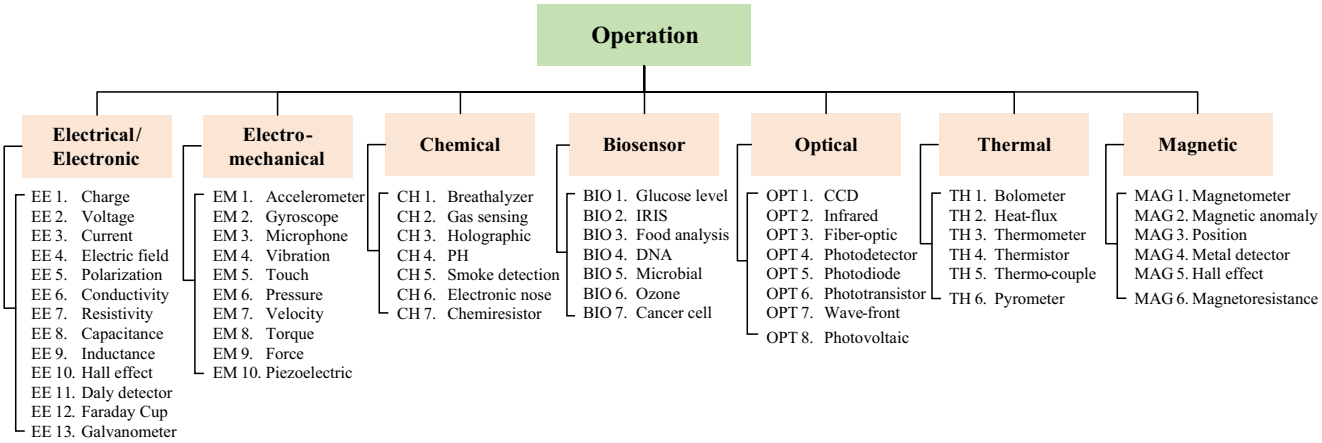

Fig. 3 Trillion sensors classification based on operating principles

dielectric constant, etc. [34]. Generally, any environmental input is converted to a voltage for measurement purpose in any electrical/electronic sensor.

b) Electromechanical The interaction of electronics, mechanics, light, or fluids working together makes up a electromechanical system. They redirect light, pump and mix fluids, and detect molecules, heat, pressure, or motion. Consumer electronics and hand-held devices use a lot of electromechanical sensors (MEMS/ NEMS) like accelerometer, gyroscope, motion, position, pressure, touch, and force sensors. MEMS like artificial retina and hearing-aid transducer are revolutionizing the healthcare applications. MEMS pressure sensors, inertial sensors, and chemical sensors have been deployed in industrial, automotive, and aerospace applications.

c) Chemical Chemical sensors respond to any particular target chemical substance present in a desired medium in order to produce a desirable signal output at any required analyte concentration [28]. Performance of the chemical sensors are limited by some features like selectivity, sensitivity, response time, packaging size, etc. Breathalyzer and pH sensors are used in biological monitoring. Gas sensors are used in area monitoring and industrial process automation. Smoke detectors are commonplace in any household/industries/offices. Toxic chemical sensors are very useful in environmental monitoring and industrial manufacturing.

d) Biosensors Biosensors are devices comprising a biological element and a physio-chemical detector that are used to detect analytes. An analyte is a substance whose chemical constituents are being identified and measured. These instruments have a wide range of applications ranging from clinical to environmental, and agricultural. The devices are also used in the food industry. Biosensors (e.g., glucose level sensors, hormone or enzyme detectors, cancer cell detectors, and blood pressure sensors) are finding more and more applications in wearable medical devices and other health-care systems.

e) Optical Optical sensors convert light rays into electronic signals. Optical sensors (e.g., photo-electric, photo-diode, photo-voltaic, and photoresistive sensors) are used in lighting control applications whereas charge-coupled device (CCD), CMOS sensors are used in video cameras. Infrared sensors can be used for temperature measurement in industrial applications. Fiber-optic sensors are used in electrical switchgear to transmit light from an electrical arc flash to a digital protective relay to enable fast tripping of a breaker to reduce the energy in the arc blast [96].

f) Thermal In thermal sensors, thermal energy is converted to electronic signals which can be used in any electronic system. Bolometers are used to detect light in the far-infrared and mm-waves. Pyrometers are used to determine temperature of any distant surface. Thermal sensors like temperature sensors, thermocouple, heat-flux sensors, and thermistor are used in industrial applications and consumer electronics alike.

g) Magnetic Magnetometers are used to detect the direction of an ambient magnetic field like the earths magnetic field. Magnetic anomaly detectors are used in the military to detect submarines. Magnetic sensors like eddy current sensors, hall effect sensors, magnetic field anomaly detectors, magneto-resistance sensors, and magnetometers are being used in mapping, positioning, and non-contact switching applications [57]. In Electric Power Steering (EPS), magnetic angle sensors and linear Hall sensors are used to measure the steering angle and steering torque.

2.3 Technology

Modern IoT/CPS systems require smart sensors where embedded microprocessors and communication modules are integral part of the sensing devices [81]. Although there are numerous sensing technologies available, considering the integration complexities, few technologies have greater impact on the overall sensor-based applications. Figure 4 summarizes some of such technologies.

a) Discrete CMOS CMOS sensors are perhaps most suitable for consumer electronics and computing devices. CMOS image sensors are already leading the global video/camera industry. CMOS temperature sensors and ionization detectors are finding their ways into standard chips/ASICs [23]. On-chip CMOS temperature sensors are used for power management. Low power consumption and the ease of integrating such sensors in system-on-chips (SoC) make them suitable for any SoC design.

b) MEMS MEMS are already a driving factor in consumer electronics and hand-held devices. Accelerometer, gyroscope, microphones, pressure, and touch sensors have revolutionized the mobile computing devices by adding more functionality and providing opportunities for numerous application development [17]. Accelerometers are also used in inertial navigation systems for air-crafts and missiles. Further, they are used to detect vibration of rotating machines. Gyroscopes are used in measuring and maintaining orientation. MEMS pressure sensors are used in the development of capacitive touch sensing applications for touchscreens.

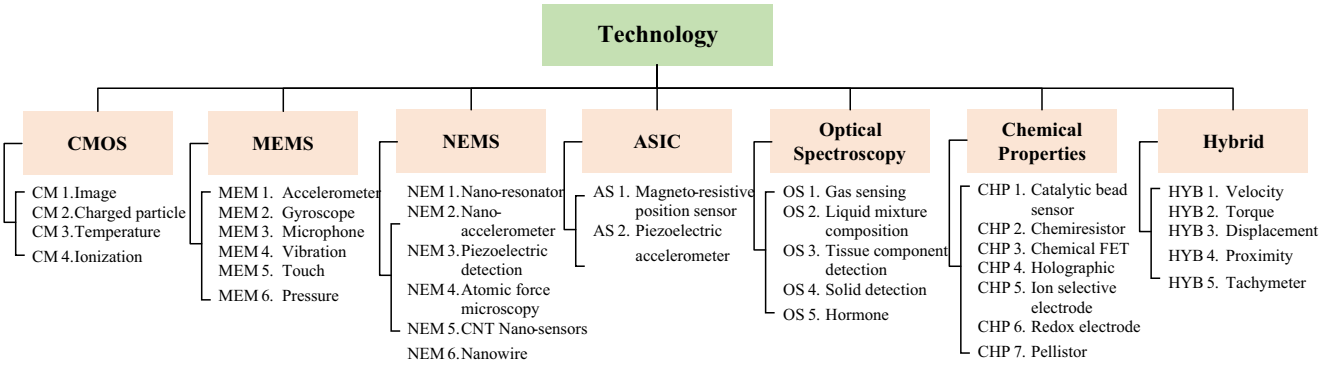

Fig. 4 Trillion sensors classification based on technologies

c) NEMS The ultra-high-frequency nano-resonators can be used in ultra-high sensitive sensing, molecular transportation, molecular separation, high-frequency signal processing, and biological imaging [14]. NEMS-based sensors are popular in medical diagnostic applications [62]. Nanowire sensors have applications in life-sciences and medicine [70]. Nanowire, nano-resonators, and nano-rods are finding their ways in complex medical diagnostic applications. Carbon nanotubes (CNT) can be used to develop electromechanical sensors for implantable devices which can be used in minimal invasive diagnosis, health monitoring, drug delivery, and many other intra-corporal tasks [50].

d) ASIC Developing application specific integrated circuits (ASIC) for specific applications can optimize the sensor performance but the associated cost can be very high which makes it suitable for applications where size and performance are the deciding factors rather than the price. Companies like Bosch are developing MEMS-based ASIC solutions for automotive industry [35].

e) Optical Spectroscopic Most liquids and gases provide unique signatures when there is an interaction with light of certain wavelength and the signature is a function of the molecular structure of the particular substance. This is the basic theory behind any optical spectroscopic sensors. These are being used in numerous applications ranging from controlling industrial processes to delineating tumor through component detection techniques [26]. Solid detection, measuring gas or liquid composition, and tissue component detection are few examples where optical spectroscopy can be used.

f) Electrochemical Electrochemical sensors are primarily used for toxic gas and oxygen detection. Each sensor is designed to be sensitive/selective to the gas it is intended to detect. Chemiresistor is the primary building block for electronic nose [95]. Pellistors are used to detect gases. Chemical FETs are field effect transistors that act as chemical sensors which can be used to detect atoms, molecules, and ions in liquids and gases. Holographic sensors can be used in distance device identification in industrial applications and anti-counterfeiting applications [89].

g) Hybrid Hybrid sensors like tachymeter, torque, velocity, and pressure sensors are widely used in automotive and control applications where multiple sensing mechanisms are integrated in an embedded control system for detection and measurement purpose.

3 Infrastructure for Sensor Based Applications

Sensors have been integrated in almost all the electronic devices we use like mobile devices, virtual reality devices, toys, stand-alone medical diagnostic devices, kitchen electrical utensils, etc. While consumer electronics is certainly the largest application of sensors right now, with the rapid growth of IoT/CPS applications, it is quite safe to say that sensor-based IoT/CPS applications will be the largest destination of sensors in the future. In order to assess the vulnerabilities in sensor-based applications, we need to analyze the system architectures in which trillions of sensors will be deployed. In this section, we present the standard architectures proposed for IoT/CPS systems. Although, the difference between IoT and CPS is not well defined and many see them as two different explanations of the same thing, IEEE has made an attempt to differentiate them in [63]. According to [63], IoT system starts from the level where a single "thing" is identified using a unique global identifier and can be accessed from anywhere, anytime. The information that the "thing" provides can be anything from sensor data or static data stored in its memory. If the "things" in this IoT system are networked together so as to

control a certain scenario in a coordinated way, then the IoT system can be considered to grow to the level of a CPS.

Since the term Internet of Things was first coined by Kevin Ashton in 1999 [38], numerous researchers have come forward with their own views about the ideal architecture for IoT. Several reference models have been proposed in an effort to come up with a generalized reference model which can be adopted by different players in the market, and thus develop products that can operate in systems built by different companies. Although, the reference models vary widely, the base-layer in any IoT reference model remains the same across all the models which deals with the issue of sensing.

Perhaps, the three-layer model proposed by Gubbi et al. was among the first IoT reference models proposed by the researchers [38]. This simplistic model is actually an extension of wireless sensor networks (WSN). It models IoT as a combination of WSN and cloud computing that can offer different applications to the end users. The bottom layer is consisted of ubiquitous sensing devices that feed data to the cloud. The applications are built on the data stored in the cloud storage as well as the directly fetched data from the sensing devices. Rafiullah et al. proposed a five-layer IoT framework [53]. They envisioned the IoT as an information network where numerous data sensed by IoT devices will be collected through the network layer in a database and applications will be built on that data. Several applications and services will be combined together to develop business models in the upper layer of this framework. In this model, the base-layer is called the perception layer which is composed of physical objects and sensors. Atzori et al. proposed another five-level IoT framework where a complex IoT systems has been decomposed into simplified applications consisting of an ecosystem of simpler and well-defined components [19]. The idea is to create many abstraction levels to hide issues that are not pertinent to a developer or a programmer. The base layer again is composed of the sensing objects which are enabled by identification, sensing, and communication technologies.

Similar architectures have been proposed for CPS. Lee et al. presented a five-layer architecture for industry 4.0 based CPS where the bottom layer incorporates sensor network and tether free communication [56]. Rad et al. proposed a four-layer CPS architecture to be used in precision agriculture where sensing is at the base layer of the framework [72]. Cisco, IBM, and Intel presented a seven-layer IoT framework in IoT World Forum 2014 that is expected to be accepted as the reference framework for IoT/CPS by the industry. In this model, data flow is usually bidirectional, but the dominant data flow direction is determined by the nature of the applications [7]. In this model, the base-layer is called Physical Devices and Controllers or Edge which includes sensors, actuators, machines, and any kind of smart devices. So, whichever framework chosen to build up any IoT system, sensing devices will be at the bottom layer of the whole architecture (Table 1).

In the Cisco IoT reference model, communications and connectivity of the IoT systems are concentrated on level-2. IoT has already kicked off with many traditional devices not fully IP-enabled or devices that require additional communication gateway devices for external connectivity. It is expected that the modern IoT devices will have integrated sensing mechanism and communication modules. Data generated by these devices will be preprocessed at the gateway and a huge chunk of the data will be dropped because of limited network resource and storage facility. Threats can come at any stage of this system—during sensing, passing the data to the gateway, preprocessing the data at the gateway, or inside the information network. The security issues in the information network are already well defined and a lot of research work has been carried out to solve these issues in the last few decades. In this paper, we are focusing on the threats that can appear at the edge devices only. As the sensing mechanism and communication modules are expected to be merged in a single IoT device, perhaps a closer look at the communication between the IoT device and the gateway will help us evaluate the threat models better.

Table 1 IoT/CPS frameworks

Three level IoT model [38]	Five level IoT model [19]	Seven level IoT model [7]	CPS 5C Architecture [56]	Four layer CPS Architecture [72]
Applications	Applications	Processes	Configuration	Application
Cloud servers	Service composition	Application	Cognition	Analyzing
Ubiquitous sensing	Service management	Data abstraction	Cyber	Networking
	Object abstraction	Data accumulation	Information conversion	Sensing
	Edge nodes	Edge computing	Smart connection	
		Connectivity		
		Edge nodes		

The connectivity level (level 2) in Cisco framework provides three basic types of data transmission: between the devices and the network, across networks and between the network, and low-level information processing at level 3 (computing at the gateway/fog computing). The edge nodes must be equipped with sensing mechanism for generating data, analog to digital conversion circuitry, and the ability to be queried/controlled over the network. The communication scenario between the IoT devices and the Internet/data server may vary based on applications. For instance, a WMS-based IoT application might use a hand-held device like a smart-phone as the gateway device [97]. A larger application like a weather monitoring system might use dedicated gateway devices for specific regions. For some applications, the gateway might transmit the raw data received and in some other cases the gateway might filter some data before transmission in order to reduce the load on the network and the data storage [7].

For communication between the IoT devices and the gateway, several technologies are available and the technologies that have caught the most attention are Bluetooth Low Energy (BLE), *ZigBee*, *Z-Wave*, Near Field Communication (NFC), *WiFi*, Thread, and Cellular (2G/3G/4G) [94]. Analyst firm ABI Research claimed that Bluetooth smart home devices will show a 75 percent growth rate between 2016 and 2021 [9]. *ZigBee* and *Thread* will lead with 34% volume share of the home automation and 29% of the smart lighting markets by this time [9]. Some protocols have been proposed for IoT communication as well most notably the *6LowPAN* protocol [65]. An IoT device designer's goal would be minimizing the area overhead, energy, and cost of the associated communication module and selection of a suitable protocol that minimizes the data overhead. As the devices will use various communication technologies, any hub designed for a smart system should be capable of handling all types of communications.

Considering the requirements of Cisco seven-level IoT reference model (Fig. 5), a standard IoT device should have a sensing mechanism, analog to digital data conversion circuitry, a communication module, and probably a security module. The security module will ensure operator trust and prevent any kind of unwanted data leakage under suspicious queries. Incorporating all these modules in a

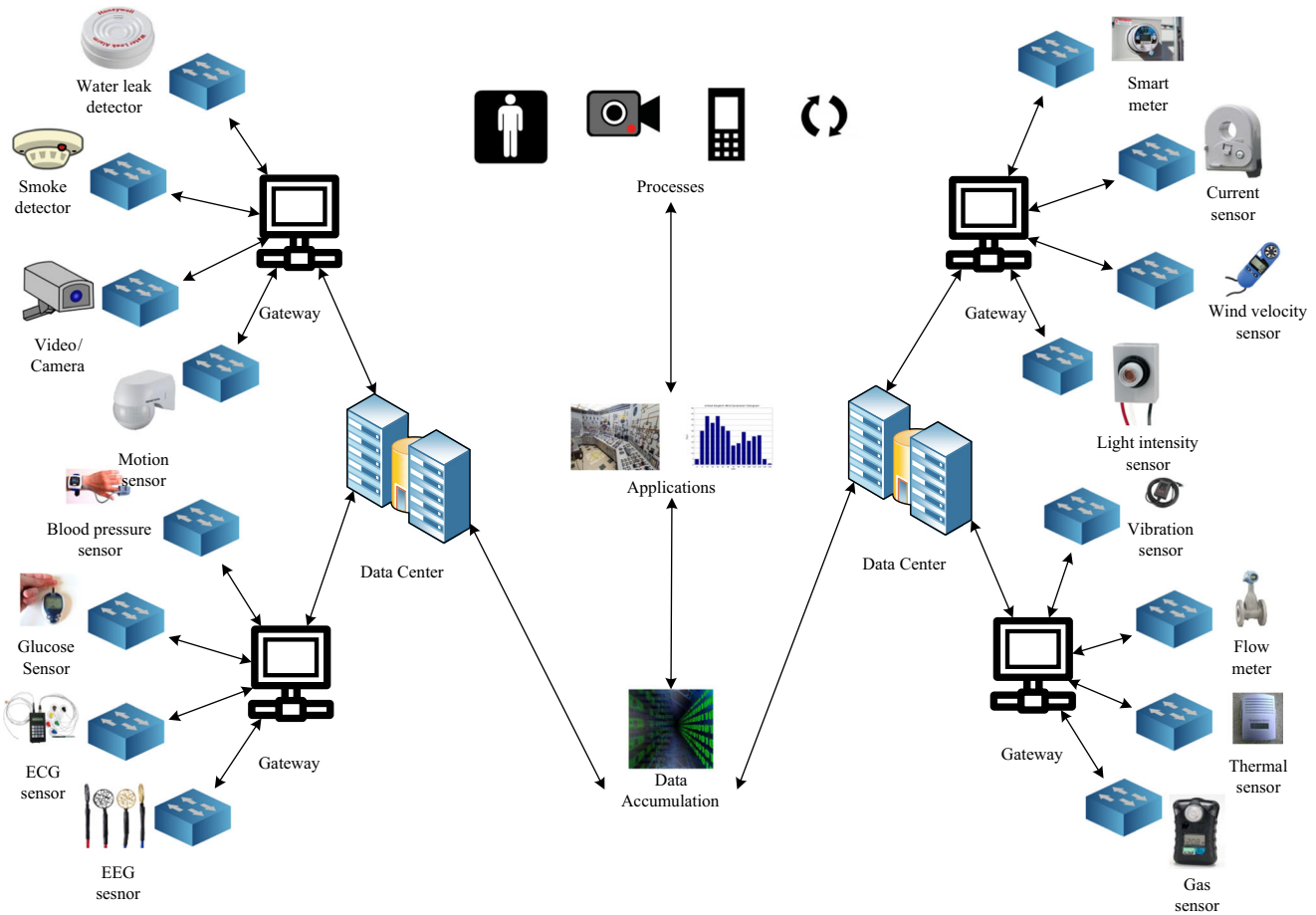

Fig. 5 Cisco seven layer IoT framework [7]

resource constrained environment presents several design challenges. The resource limitations and associated design challenges are discussed in the following section.

4 Limitations and Challenges

Recent studies have shown that modern IoT/CPS sensor nodes are severely resource constrained which limits the ability of these devices to use standard cryptographic protocols to communicate securely. Trappe et al. showed that the power constraint in IoT edge devices limits the encryption/encoding functionality of the sensor nodes which leads to poorly encrypted communication or no encryption at all [87]. In a study, HP revealed that almost 70% of IoT devices they tested did not encrypt communications to the Internet and the local network, while half of the device's mobile applications performed unencrypted communications with the cloud, the Internet, and local network [73]. Almost 60% of the devices under study did not use encryption while downloading software updates. Symantec also found 19% of the devices under test to use no encryption during communication with the cloud server or the back-end applications and even fewer use encryption while communicating in the local network [21]. These lead to opportunities for the adversaries to attack such systems.

Absence of cryptography in communication results in inadequate security measures in the edge devices. Consequently, ensuring data integrity, maintaining confidentiality of the communication, authenticating the edge devices, and controlling access to the devices become very challenging. The devices might be vulnerable to different kinds of denial of service (DoS) attacks [90]. Sleep deprivation attacks can severely affect the operation of the IoT/CPS application by draining the energy source of power constrained edge devices [22]. Attacks such as hello flooding, Sinkholes, Wormholes, Sybil attack, etc. which are prevalent in any wireless sensor network will also be present in any IoT/CPS application [52, 61, 71, 80]. In gateway-centric model of IoT/CPS, security measures would most likely have to be implemented in the gateway devices to pro-vide security against these attacks due to the resource constraints in the IoT/CPS edge devices. These security threats are well documented in the domain of wireless sensor networks. One can take a look at these articles to have a greater understanding of those attacks which is clearly out of scope of this paper.

In this section, we are going to focus on the limitations of standard IoT devices and the threats that might arise due to large volume of sensors in both—the software and the hardware levels.

4.1 Resource Constraints

In most IoT/CPS applications, sensors are placed in large geographical areas and associated cost prohibits regular maintenance. Consequently, when the sensors are deployed in the field, they are expected to operate uninterrupted for a long period of time. In order to support large scale adoption, these sensors are severely budget constrained which in turn result in the integration of small batteries, low end processors and very limited memories in IoT/CPS sensor-based edge devices [87]. Operating on a small battery for a long period of time presents some unique design challenges which have forced the designers to consider energy harvesting from the nature, operating the devices in low energy sleep state majority of the time, and avoiding energy intensive cryptographic computations. The processors offered in the market for IoT sensor nodes are mostly micro-controllers with limited capabilities, specialized for a specific task, and designed for mass production and low cost. Cycle intensive raw data processing at the sensor nodes is not possible due to the power constraints.

Avoiding cryptographic computations altogether in these resource constrained IoT/CPS sensor nodes makes this system vulnerable to all sorts of cyber attacks. The following studies have shown that the seemingly harmless IoT data can be used to extract useful information about the overall system. Inter-dependency of different components in an IoT environment offer adversaries unique ways to attack the system. Tampering the data generated by a temperature sensor might be used to sabotage fire alarm in a smart home. Attackers have successfully breached the security of an automotive system through passive tire pressure sensors. In another study, attackers have passively read wireless electric meters at distances of hundreds of meters, and thus have developed a detailed pattern of the resident energy use which is clearly a breach of privacy. Such observations have encouraged the development of light-weight cryptographic schemes which can be used in low resource communication, specially for the low-end IoT devices.

In order to facilitate large-scale adoption of the sensors in diverse applications, the sensor nodes have to be low-cost devices. So, the sensor itself, the associated networking and processing hardware, and the firmware—all of them have to be produced under cost constraints. The expected cost for a sensor node might be as low as 10 cents [24]. In order to support low power operations and budget constraints, the area overhead of the overall sensing platform has to be as small as possible.

The technologies that might be used to produce the sensor nodes for IoT/CPS applications can vary widely

as shown in Section 2.3. The power, area, and cost constraints put a limitation on the suitable technologies for low-end IoT/CPS sensor nodes. Typically, a sensor node consists of four basic components—a sensing unit, processor unit, transceiver unit, and a power management unit. Incorporating them in a single chip to develop an ASIC can optimize the performance and power consumption, but the development cost can be too high to justify such implementations. The security of the system can be provided through a separate hardware unit which might increase the cost of the sensor nodes significantly. Software implementation of the cryptographic primitives is a cost effective solution to provide security in the sensor nodes [76]. But limited processing power, energy resource and available memory—limit the capability of the sensor nodes to implement highly secure cryptographic primitives on such devices as discussed in Section 4.2.

4.2 Low-Resource Communication and Computation

Sensors in an IoT/CPS network generates real time data, and sends it to a designated server through gateways. The gateways have ample resources to deploy required security protocols to send the data to the server over the public Internet, whereas the edge nodes in an IoT/CPS system are resource constrained which prohibits them from using standard security protocols. Any secure data transfer protocol must have the following properties: confidentiality, message integrity, and end-point authentication [55].

- *Confidentiality:* Only the sender and the receiver should be able to extract the meaning of the transferred data. Symmetric key cryptography and public key cryptography are two widely used methods for ensuring confidentiality in communication. This can be achieved through symmetric ciphers (e.g., advanced encryption standard (AES) [29] and 3DES) and asymmetric ciphers (Rivest-Shamir-Adleman
  (RSA) [75] and Elliptic curve cryptography (ECC) [47]).
- *Message Integrity:* The receiver must be able to verify whether the message has been altered or not. Message authentication codes (MAC) are generally used for the verification of message integrity. Keyed-hash message authentication code (HMAC [66]) is a MAC that uses a secure hash function (e.g., SHA-2 and SHA-3 [67]).
- *End-point Authentication:* The receiver must verify that the request was initiated by the trusted sender (not by an adversary). This can be achieved through digital signatures [59] generally constructed by using RSA or ECC.

All these cryptographic primitives are computationally heavy which require large processing power and energy. Hardware implementation of the above cryptographic primitives with a separate chip can be prohibitive for a low-end IoT/CPS sensor node because of the cost constraints. So, a software implementation of the security primitives is more practical. However, the computing capabilities of a sensor node are very limited: a typical node has a 8MHz micro-controller with less than 128KB of instruction memory and approximately 10KB of RAM memory [76]. Therefore, it is necessary to analyze how the existing primitives could perform over these highly-constrained nodes. Table 2 summarizes the design overhead of different cryptographic primitives.

Resource constraints in IoT/CPS sensor nodes have fueled the development of low resource communication and computation techniques for these applications. RFID tags are a prime example of resource constrained devices. Most RFID researchers believe that the industry requires simple and low cost RFID tags with limited number of logic gates which reduces the cryptographic capability of such devices [20, 51]. Several light-weight RFID protocols have been proposed and [32, 49, 54, 58, 82, 83, 88] are just to name a few. Most of these protocols utilize cryptographic hash functions, random number generators, and XOR functions which are light-weight solutions compared to other computationally expensive symmetric key and public key cryptographic primitives.

Henrici et al. have presented a protocol that uses cryptographic hash functions and XOR operators to encrypt the communication between the RFID tag and the reader and a random number generator and hash functions to authenticate the reader to the tags [49]. Lim et al. proposed a protocol where the reader and the RFID tag, both use random number generators, hash functions, and XOR primitives to authenticate each other [58]. Tan et al. proposed a server-less authentication protocol that also utilizes a known hash function between the reader and the tags, and XOR primitives. All these protocols are light-weight but have some security flaws which can be

Table 2 Software/Hardware implementation overhead of standard crypto-primitives

Crypto-primitive	Gate Count	Code Size (Bytes)
3DES	5504 [78]	–
AES	1100 [86]	840 [86]
ECC	13800 [46]	2166 [46]
RSA	861 [64]	1073 [46]
SHA-3	10500 [12]	1500 [37]

manipulated by the adversaries to attack the system. For instance, the protocol proposed by Henrici et al. maintains a session number to synchronize the tag and the reader which can be easily manipulated by a malicious attacker by interrogating the tag in a middle step of the authentication process, and thus desynchronizing the tag and the reader [49]. In Lim et al.'s protocol, total number of authentication session requests are limited which makes it vulnerable to denial-of-service (DoS) attacks [58]. In the protocol proposed by Tan et al., the tag returns a static form of data based on its ID and a secret which can be utilized to track the tag by any adversaries. These naive security flaws have kept the development of such protocols ongoing [83].

PUFs have emerged as a low-cost solution for cryptographic key generation, and thus have become popular in developing some PUF-based communication protocols. Ruhrmair et al. have proposed a security tool named SIMPL Systems which can be used for device identification and message authentication [77]. This system is based on the concept of public PUF where strong PUF primitives in each device are used to produce random nonces for different challenges and a mathematical model of the system and associated simulation model is made public for identification and message authentication applications. The central idea behind the system is—a PUF hardware generates a response far quickly compared to any computer generated model and the PUF itself is unclonable in nature, so an adversary can never produce an exact physical match of the PUF which ensures the security of the system.

Secure communication requires end-point authentication and there are several PUF-based authentication protocols in the literature for resource constrained sensor nodes of IoT/CPS applications. Most of these protocols work in two phases. In the first phase, the devices are enrolled in a secure database with the PUF responses which is called the enrollment phase. In the second phase, the devices are deployed in the field where they are exposed to physical attacks. The devices are authenticated based on the PUF responses over an insecure communication channel. Considering the device constraints, these protocols have been kept light-weight. The unreliable nature of PUF outputs, the vulnerabilities of these sensor nodes to physical attacks, and ad-hoc nature of these protocols have resulted in many security flaws which can be manipulated by the adversaries. In [30], Delvaux et al. presented the security flaws of 19 different strong PUF-based authentication protocols which indicates that developing an ideal low-cost authentication protocol for IoT/CPS sensor nodes is still a challenge.

In order to save power and operate on small batteries for large period, application specific processors have been built for IoT applications. Approximate computing for low-end IoT node processors have been considered to save power [36]. Re-configurable processors with limited functionalities have been considered as well which can be optimized for power consumption for specific applications [60].

4.3 Trust Issues in Sensor Supply Chain

With the advent of globalization in the product manufacturing and its resulting horizontal integration, it is becoming increasingly difficult to ensure the authenticity of electronic systems. Today's electronic systems are assembled all across the globe, and consist of components sourced from different parts of the world. It is now virtually impossible to find out the origin of electronic products, and track their route in the supply chain. We have observed this far-reaching penetration of non-authentic systems and counterfeit parts into the electronics supply chain [39, 40, 42, 84, 85].

Typically an electronic supply chain goes through the following processes—design, manufacturing, distribution, and resign/end-of-life. In every process, there can be multiple independent entities involved with different motives which complicates the supply chain and exposes multiple points of vulnerabilities. The supply chain of IoT/CPS sensor devices will be the same as well. From design specifications, the original system designer will develop the hardware and firmware for the sensor nodes and will invest on research and development of the product. They might integrate designs or chips from third party entities into their design. The finalized design will go to the foundries or assemblies for manufacturing. The manufactured products will come to the market through the distributors. Moreover in the future, trillions of different sensors will produce tremendous amount of electronic waste when the product lifetime finishes which might be used for recycling afterwards by different entities.

In this complicated supply chain, any of the involved entities might try to manipulate the vulnerabilities in order to gain some unfair financial benefits. For example, a rogue designer in the design house might put a bug into the design intentionally, or a third party IP vendor might put Trojans in their IPs, or the design house might overuse third party IPs, or steal the design concept and sell it to other competitors. Design can be stolen through reverse engineering as well. A distributor might sell sensors with lower grades after remarking it with a higher grade. The demand for newer low-cost and resource constrained embedded systems is going to increase which will force the system design companies to look for low-cost chips through the semiconductor supply chain. Recycled sensors and associated networking and processing chips collected from e-waste might find their ways to the supply chain because of lower cost.

Design complexity and exponentially growing market demand will result in more piracy. Avoiding R&D and design cost, counterfeiters will be able to supply low cost sensors, processors, and networking chips to the IoT market where lower device cost dictates widespread adoption. Counterfeit sensors in an IoT/CPS environment might compromise the security of the system, can be used to leak valuable information, or can disrupt operation through unexpected device failure. In the following section, we have discussed about different ways that the adversaries might use to corrupt the sensor supply chain with counterfeit products.

4.3.1 Piracy

Competitive market and rising demands for IoT devices will put much pressure on the design companies, and time-to-market for IoT/CPS products will shrink considerably over time. Sensor-based applications will require bulk amount of sensors and associated chips to be supplied in a very short time which might give rise to design cloning and piracy. An untrusted manufacturing unit can pirate the design details of a sensor during manufacturing, and thus avoid R&D cost. A design can also be reconstructed through reverse engineering. The stolen design can be modified to insert malicious circuits into the design. In today's IP-based SoC design, the system integrator can steal/overuse/modify the third party IPs and thus gain unfair financial benefits [27, 43, 44].

An adversary can penetrate the IoT/CPS market with sensors that have been rejected after manufacturing tests, or have been remarked with a higher grade. We have observed rejected ICs in defense supply chain [85]. This is very plausible that we will see rejected sensors in our critical applications, such as smart grid. Due to lower cost, these sensors might attract the system design companies, especially those who produce low-end devices for sensor-based applications. In addition, an adversary can mark the sensor devices with a higher grade than they are in reality for financial benefits. Such remarking process can cause severe risk if the sensors are operated in harsh environments where a real higher grade sensor is necessary. We also have seen a similar trend in the IC supply chain where new ICs are often remarked with higher grade to make profit [85]. Remarked sensors in sensor-based IoT/CPS applications which are operated in severe environmental conditions might cause system failure in critical conditions.

The diversity of IoT-based applications is already giving rise to small-scale companies that specialize on specific products. Specially smart systems and healthcare solutions are so varied in nature that these are encouraging the development of different start-ups [8]. Moreover, modern self-driving cars are incorporating multiple IoT solutions to enable its self-driving capabilities and continuously improving the system performance. As the original component manufactures (OCM) continuously improves the specification, performance and cost of their products, we believe similar situation, like semiconductor industry, will occur in near future. This can open new financial opportunities for the counterfeiters to pirate the design, manufacture chips, and make a stock of such chips which they can sell at a very high rate when the original chips are discontinued.

4.3.2 Reverse Engineering

Considering the design complexities of a low-end resource constrained sensor node and probable large-scale demand for such devices in sensor-based applications, reverse engineering will attract counterfeiters to gain undue profits. Avoiding the R&D cost through reverse engineering, counterfeiters might be able to supply these sensors and associated networking and processing chips at a lower cost than the original manufacturers which will result in a huge loss of revenue for the industry. We have seen a similar trend for electronic systems [39, 84]. IoT/CPS sensor nodes are basically embedded systems with sensing and communicating capabilities (discussed in Section 3). As stated earlier, the exponential growth of new IoT solutions in the healthcare and smart systems domain, and demand for chips fabricated in older technologies in the field of automobiles, industrial control systems, and airplanes will justify the cost associated with reverse engineering.

Several destructive and non-destructive methods are available today to produce a 3D layout of an IC or printed circuit boards (PCB) with superfine resolution. Scanning electron microscope (SEM) or transmission electron microscopes (TEM) can be used to capture the inner layer of any integrated circuit. X-ray tomography can be used to extract 3D layout of a fully functional PCB [16]. Such cloning has been performed successfully even in academic research laboratory for feasibility studies [15]. Full chip layout can be constructed by extracting layout of each layer of the design through etching and scanning with electron microscopes. Typical ICs today incorporates more than 50 layers which means after destructing a few chips, a full chip design can be engineered through this process. The imaging technology associated with the destructive methods of reverse engineering is far cheaper than the other non-destructive methods which makes it a cheaper option for the counterfeiters.

4.3.3 Recycling

A standard IoT/CPS sensor node incorporates sensor devices, embedded processor, and memory and any of these devices can come through recycling. Recycling ICs

from electronic waste has become a huge problem [40–42, 45, 85]. These recycled ICs have lesser remaining useful lifetime than any fresh ICs and the process through which they are collected also reduce their lifetime further. These ICs come to the electronic supply chain through the grey market, and incorporating them in IoT/CPS infrastructure can cause frequent chip failure, and thus it can increase the cost of system maintenance. Low-cost recycled sensors and associated chips might find their ways into large scale sensor-based applications. As these applications are expected to perform uninterrupted for a long period of time to reduce maintenance cost, shorter lifetime of the recycled chips might disrupt the operation of such applications. Using recycled chips in low-cost medical devices can cause false diagnosis which can lead toward severe health-risk.

4.4 Physical Attacks

As the sensor nodes are spread geographically in most IoT/CPS applications, they can also be prone to physical attacks. The sensor data can be corrupted by manipulating the sensor environment by any adversary. Attackers can physically damage IoT devices to disrupt the availability of service. As in a connected environment, the sensor data can be used to control some other applications, these dependent applications can be attacked through physical attacks on the sensor nodes. For example, if a sprinkler system in a smart-home environment operates based on the temperature feedback from a temperature sensor, an adversary can manipulate the sensor environment to feed a false temperature data into the sprinkler system, and thus he can turn it on. In an industrial IoT application, manipulating a few sensor data can disrupt the whole control system if necessary security measures are not taken.

5 Future Directions

The resource constrained IoT/CPS sensor nodes are vulnerable to both software and hardware-based attacks. The limited computational power, low energy resource, and memory do not allow these devices to use standard cryptographic protocols during data communication and edge device authentication which have been discussed in Section 4. Therefore, these sensor nodes are vulnerable to many software-based attacks like data sniffing, false packet injection, sleep deprivation, DoS attacks, etc. [11]. Piracy, reverse engineering, recycling, and tampering are the forms of hardware-based attacks that pose severe threats to the security of such systems which have been presented in Section 4.3. Among trillions of sensors, even a very small percentage of compromised devices can be used to target different systems, and can cause significant damage to the applications. Hence, any solution to secure these sensors applications must be comprehensive that ensure security at both the software and the hardware-level.

Most of the light-weight encryption schemes and communication protocols which have been developed for IoT/CPS sensor nodes have loopholes due to resource limitations. These loopholes can be manipulated by an adversary to attack such systems which has been discussed briefly in Section 4.2. Authentication of the sensor nodes, and ensuring integrity of the generated data is still a challenge. Developing encryption schemes that require low power, memory and computational resources is still an ongoing research area. The sensor nodes incorporates small batteries and they are expected to operate uninterrupted for a long period of time. Consequently, power consumption has to be minimized in every possible steps—during data generation and data transmission. The associated protocols have to be very light-weight. But, avoiding security features altogether in the sensor nodes, which is the current trend in IoT system development considering the generated data is of limited value to the attackers, can lead to disastrous effects which have been shown by recent studies. Developing light-weight and secure communication protocols is a challenge which has to be solved in order to provide a secure and trusted IoT/CPS environment.

Identification of products in retail service through RFID tags is very popular nowadays, but the associated RFID communication protocols are vulnerable to external attacks. These attacks are mentioned in Section 4.2. So, developing RFID protocols which can ensure that an adversary can not read the tags, or manipulate the protocol to track the particular object is of utmost importance.

The volume of data the IoT/CPS sensor nodes can produce, can overwhelm the current Internet infrastructure. Processing the large amount of raw sensor data in the server seems an attractive scenario but considering the limitations of battery power, limited available band-width, and compute cycle intensive algorithms, this concept lacks practicality. So, ultra-low-power processing techniques have to be developed for the sensor nodes so that instead of transmitting raw sensor data, the nodes can transmit a subset of the data which can still carry all the required information.

IoT and CPS systems have accelerated the growth of number of connected sensor nodes exponentially. Ericsson predicts 28 billions of connected devices by 2021, whereas other sources also predict similar figures [68]. Even a small percentage of counterfeit devices, like 0.01%, means more than 20 millions of compromised devices which can be manipulated by the adversaries to attack these connected applications. The horizontal integration model of current global IC supply chain has vulnerabilities. Exploiting these vulnerabilities, the adversaries have polluted the IC supply chain with cloned, recycled, remarked, and rejected ICs

which has been discussed in Section 4.3. Designing a resource constrained sensor node is more complex than designing a standard system-on-chip for mobile devices. The huge demand for the sensor nodes for trillion sensors applications, and the associated design complexity might give rise to design cloning, reverse engineering, and IC overproduction by the foundries. Developing methods to secure the IC supply chain is an area where substantial research work is necessary.

Identification and authentication of each sensor node connected in any IoT/CPS application with unclonable IDs is one solution which has been considered to ensure IC supply chain security. PUFs have emerged as a low cost solution for creating unclonable IDs. But the unreliability in standard PUF outputs have limited their applications. Developing authentication protocols that can deal with unreliable IDs is necessary. Developing new PUF architectures, or exploiting the current architectures to increase the reliability is an ongoing research direction.

If sensors are embedded everywhere throughout the global supply chains—in vehicles, wearables, auto-ID tags, machines, store shelves, cotton fields, warehouses, barcode scanners, clothing fabrics, drones, industrial robots, shipping containers—we are essentially heading for the trillion sensor supply chain. With a trillion sensors constantly gathering data everywhere, we will inch closer to a situation where managers will be able to know anything they want to know about their supply chains anytime and anywhere. The greater visibility of the supply chain can be utilized to develop applications that can take informed decisions to optimize the supply chain operation. For instance, Yang et al. provided a comprehensive solution for securing IC supply chain through increasing the traceability of the ICs through RFID tags [91–93]. Similar implementations are expected in other industries as well.

6 Conclusion

In this paper, we have presented an overview of TSensors applications, current infrastructure, and challenges ahead. Large-scale deployment of sensors demand simplification of associated hardware for cost minimization which in turns results in numerous security vulnerabilities in such systems. Resource constraints in the edge nodes of such applications, their impacts on secure communication, and system security have been discussed. In addition, we have presented all different vulnerabilities in the sensor supply chain that can potentially be exploited by an adversary to gain access of a secure system. Adequate security measures need to be taken to secure the sensor supply chain. We need to be proactive in facing these challenges rather than waiting for the attacks to happen in the near future.

Acknowledgements The work of Ujjwal Guin was supported in part by the Intramural Grants Program from Auburn University and the work of Mark Tehranipoor was supported in part by National Science Foundation under grants CNS-1558516 and ECCS 1610075.

References

1. Increasing Food Production with the Internet of Things. Intel, Case Study
2. Kansas City & Cisco: Engaging the 21st Century Citizen. Cisco, Case Study
3. Automating Field Service with the Internet of Things (IoT). Cisco, Case Study
4. Predix—The platform for the Industrial Internet. GE, Case Study
5. Smart Home Technology Lets Seniors Age-in-Place Gracefully at Breton Homes North. Leviton Manufacturing Co., Inc.
6. Kurt Salmon RFID in Retail Study 2016. Kurt Salmon, Case Study
7. (2014). The Internet of Things Reference Model. Cisco Systems
8. 64 healthcare iot startups in patient monitoring, clinical efficiency, biometrics, and more. https://www.cbinsights.com/research/iot-healthcare-market-map-company-list/
9. Iot to account for 28% of wireless connectivity ic market by 2021; driven by fast-growing smart home, wearables, and beacons. https://www.abiresearch.com/press/iot-account-28-wireless-connectivity-ic-market-202/
10. Smart systems and services growth opportunities. http://harborresearch.com/wp-content/uploads/sites/8/2016/02/HRI_ThingWorx-Reprort_Smart-Services-Business-Model-Innovation.pdf
11. Abomhara M et al (2015) Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mobility 4(1):65–88
12. Akin A, Aysu A, Ulusel OC, Savaś E (2010) Efficient hardware implementations of high throughput sha-3 candidates keccak, luffa and blue midnight wish for single-and multi-message hashing. In: Proceedings of the 3rd International Conference on Security of Information and Networks, pp. 168–177. ACM
13. Annunziata M, Evans PC (2012) Industrial internet: pushing the boundaries of minds and machines. General Electric
14. Arash B, Jiang JW, Rabczuk T (2015) A review on nanomechanical resonators and their applications in sensors and molecular transportation. Appl Phys Rev 2(2):021,301
15. Asadizanjani N, Shahbazmohamadi S, Tehranipoor M, Forte D (2015) Analyzing the impact of x-ray tomography for non-destructive counterfeit detection. In: Proc. Int. Symp. Testing Failure Anal., pp 1–10
16. Asadizanjani N, Shahbazmohamadi S, Tehranipoor M, Forte D (2015) Non-destructive pcb reverse engineering using x-ray micro computed tomography. In: 41st International symposium for testing and failure analysis, ASM, pp 1–5
17. Asin A, Gascon D (2012) 50 sensor applications for a smarter world. Libelium Comunicaciones Distribuidas, Tech. Rep
18. Association SI et al (2015) International technology roadmap for semiconductors 2.0. http://public.itrs.net/
19. Atzori L, Iera A, Morabito G (2010) The internet of things: A survey. Comput Netw 54(15):2787–2805
20. Avoine G, Oechslin P (2005) Rfid traceability: A multilayer problem. In: Financial Cryptography, vol 3570, pp 125–140. Springer
21. Barcena MB, Wueest C Insecurity in the internet of things
22. Bhattasali T, Chaki R, Sanyal S (2012) Sleep deprivation attack detection in wireless sensor network. arXiv preprint arXiv:1203.0231
23. Boppel S, Lisauskas A, Mundt M, Seliuta D, Minkevicius L, Kasalynas I, Valusis G, Mittendorff M, Winnerl S, Krozer V et al

(2012) Cmos integrated antenna-coupled field-effect transistors for the detection of radiation from 0.2 to 4.3 thz. IEEE Trans Microwave Theory Tech 60(12):3834–3843
24. Bryzek J (2013) Roadmap for the trillion sensor universe. Berkeley, CA
25. Bryzek J (2014) Trillion sensors: Foundation for abundance, exponential organizations, internet of everything and mhealth, SENSOR MAGAZINE, Trade Journal Rep
26. Conde OM, Eguizabal A, Real E, López-Higuera JM, Garcia-Allende PB, Cubillas AM (2013) Optical spectroscopic sensors: From the control of industrial processes to tumor delineation. In: 2013 6th International Conference on Advanced Infocomm Technology (ICAIT), p 91–92. IEEE
27. Contreras GK, Rahman MT, Tehranipoor M (2013) Secure split-test for preventing ic piracy by untrusted foundry and assembly. In: 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), p 196–203. IEEE
28. Council NR et al (1995) Expanding the vision of sensor materials. National Academies Press, Washington
29. Daemen J, Rijmen V (2013) The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, Berlin
30. Delvaux J, Peeters R, Gu D, Verbauwhede I (2015) A survey on lightweight entity authentication with strong pufs. ACM Comput Surv 48(2):26
31. Diamandis PH, Kotler S (2012) Abundance: The future is better than you think. Simon and Schuster, New York
32. Dimitriou T (2005) A lightweight rfid protocol to protect against traceability and cloning attacks. In: 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005., pp 59–66. IEEE
33. Duffy J At&t allies with cisco, ibm, intel for city iot. Network World
34. Farhangi H (2010) The path of the smart grid . IEEE Power Energ Mag 8(1):18–28
35. Fischer A Bosch designs application-specific integrated circuits for mems sensors in dresden. http://www.bosch-presse.de/pressportal/de/en/bosch-designs-application-specific-integrated-circuits-for-mems-sensors-in-dresden-42032.html
36. Gao M, Wang Q, Arafin MT, Lyu Y, Qu G (2017) Approximate computing for low power and security in the internet of things. Computer 50(6):27–34
37. Gauravaram P, Knudsen LR, Matusiewicz K, Mendel F, Rechberger C, Schläffer M, Thomsen SS (2009) Grøstl-a sha-3 candidate. In: Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum für Informatik
38. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (iot): A vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660
39. Guin U, Bhunia S, Forte D, Tehranipoor M (2016) Sma: A system-level mutual authentication for protecting electronic hardware and firmware. IEEE Transactions on Dependable and Secure Computing
40. Guin U, DiMase D, Tehranipoor M (2014) Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. J Electron Test 30(1):9–23
41. Guin U, Forte D, Tehranipoor M (2016) Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling. IEEE Trans Very Large Scale Integr VLSI Syst 24(4):1233–1246
42. Guin U, Huang K, DiMase D, Carulli J, Tehranipoor M, Makris Y (2014) Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. Proc IEEE 102(8):1207–1228
43. Guin U, Shi Q, Forte D, Tehranipoor M (2016) FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs. In: ACM Transactions on Design Automation of Electronic Systems (TODAES)
44. Guin U, Tehranipoor M (2017) Obfuscation and encryption for securing semiconductor supply chain. In: Hardware Protection through Obfuscation, pp 317–346. Springer
45. Guin U, Zhang X, Forte D, Tehranipoor M (2014) Low-cost on-chip structures for combating die and ic recycling. In: Proceedings of the 51st Annual Design Automation Conference, pp 1–6. ACM
46. Gura N, Patel A, Wander A, Eberle H, Shantz SC (2004) Comparing elliptic curve cryptography and rsa on 8-bit cpus. In: CHES, vol 4, pp 119–132. Springer
47. Hankerson D, Menezes AJ, Vanstone S (2006) Guide to elliptic curve cryptography. Springer Science & Business Media, Berlin
48. Hartwell P, Williams R (2010) Hp cense: sensor networks and the pulse of the planet. Prezentacja dostępna na http://www.slideshare.net/hewlettpackard/hp-cense-sensor-networks-and-the-pulse-of-the-planet
49. Henrici D, Muller P (2004) Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In: Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on, pp. 149–153. IEEE
50. Hierold C, Jungen A, Stampfer C, Helbling T (2007) Nano electromechanical sensors based on carbon nanotubes. Sensors Actuators A Phys 136(1):51–61
51. Juels A (2006) Rfid security and privacy: A research survey. IEEE J Sel Areas Commun 24(2):381–394
52. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Netw 1(2):293–315
53. Khan R, Khan S, Zaheer R, Khan S (2012) Future internet: the internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology (FIT), pp 257–260. IEEE
54. Kulseng L, Yu Z, Wei Y, Guan Y (2010) Lightweight mutual authentication and ownership transfer for rfid systems. In: INFOCOM, 2010 Proceedings IEEE, pp 1–5. IEEE
55. Kurose JF, Ross KW (2009) Computer networking: a top-down approach, vol 4. Addison Wesley, Boston
56. Lee J, Bagheri B, Kao HA (2015) A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Lett 3:18–23
57. Lenz J, Edelstein S (2006) Magnetic sensors and their applications. IEEE Sensors J 6(3):631–649
58. Lim TL, Li T, Gu T (2008) Secure rfid identification and authentication with triggered hash chain variants. In: 14th IEEE International Conference on Parallel and Distributed Systems, 2008. ICPADS'08., pp 583–590. IEEE
59. Locke G, Gallagher P (2009) Fips pub 186-3: Digital signature standard (dss). Federal Inf Process Standards Publ 3:186–3
60. Ma N, Zou Z, Lu Z, Zheng L, Blixt S (2014) A hierarchical reconfigurable micro-coded multi-core processor for iot applications. In: 2014 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip (ReCoSoC), pp 1–4. IEEE
61. Meghdadi M, Ozdemir S, Güler I. (2011) A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. IETE Tech Rev 28(2):89–102
62. Michalewicz MT, Sasse A, Rymuza Z Quantum tunneling nems devices for bio-medical applications
63. Minerva R, Biru A, Rotondi D (2015) Towards a definition of the internet of things (iot). IEEE Internet Initiative (1)

64. Miyamoto A, Homma N, Aoki T, Satoh A (2011) Systematic design of rsa processors based on high-radix montgomery multipliers. IEEE Trans Very Large Scale Integr VLSI Syst 19(7):1136–1146
65. Mulligan G (2007) The 6lowpan architecture. In: Proceedings of the 4th workshop on Embedded networked sensors, pp 78–82. ACM
66. (2008). NIST: FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC)
67. (2012). NIST: FIPS PUB 180-4: Secure Hash Standard
68. Nordrum A (2016) Popular internet of things forecast of 50 billion devices by 2020 is outdated. IEEE Spectrum 18
69. OBILE W (2016) Ericsson mobility report
70. Patolsky F, Zheng G, Lieber CM (2006) Nanowire sensors for medicine and the life sciences
71. Perrig A, Stankovic J, Wagner D (2004) Security in wireless sensor networks. Commun ACM 47(6):53–57
72. Rad CR, Hancu O, Takacs IA, Olteanu G (2015) Smart monitoring of potato crop: a cyber-physical system architecture model in the field of precision agriculture. Agric Agric Sci Procedia 6:73–79
73. Rawlinson K Hp study reveals 70 percent of internet of things devices vulnerable to attack. http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WUrrwWgrKM8
74. Reisinger D. Amazon's cashier-free store might be easy to break. http://fortune.com/2017/03/28/amazon-go-cashier-free-store/
75. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
76. Roman R, Alcaraz C, Lopez J (2007) A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. Mobile Netw Appl 12(4):231–244
77. Rührmair U (2009) Simpl systems: On a public key variant of physical unclonable functions. IACR Cryptology ePrint Archive 2009:255
78. Satoh A, Morioka S (2003) Hardware-focused performance comparison for the standard block ciphers aes, camellia, and triple-des. In: International Conference on Information Security, pp 252–266. Springer
79. Saxena A (2016) Digital twin enabling phm at industrial scales
80. Singh VP, Jain S, Singhai J (2010) Hello flood attack and its countermeasures in wireless sensor networks. IJCSI Int J Comput Sci Issues 7(11):23–27
81. Spencer BF, Ruiz-Sandoval ME, Kurata N (2004) Smart sensing technology: opportunities and challenges. Struct Control Health Monit 11(4):349–368
82. Sun HM, Ting WC (2009) A gen2-based rfid authentication protocol for security and privacy. IEEE Trans Mob Comput 8(8):1052–1062
83. Tan CC, Sheng B, Li Q (2008) Secure and serverless rfid authentication and search protocols. IEEE Trans Wirel Commun 7(4):1400–1407
84. Tehranipoor M, Guin U, Bhunia S (2017) Invasion of the hardware snatchers. IEEE Spectr 54(5):36–41
85. Tehranipoor M, Guin U, Forte D (2015) Counterfeit Integrated Circuits: Detection and Avoidance. Springer, Berlin
86. Tillich S, Herbst C (2008) Boosting aes performance on a tiny processor core. Topics in Cryptology–CT-RSA 2008:170–186
87. Trappe W, Howard R, Moore RS (2015) Low-energy security: Limits and opportunities in the internet of things. IEEE Secur Priv 13(1):14–21
88. Vajda I, Buttyán L et al (2003) Lightweight authentication protocols for low-cost rfid tags. In: Second Workshop on Security in Ubiquitous Computing–Ubicomp, vol 2003
89. Vasconcellos FDC, Yetisen AK, Montelongo Y, Butt H, Grigore A, Davidson CA, Blyth J, Monteiro MJ, Wilkinson TD, Lowe CR (2014) Printable surface holograms via laser ablation. ACS Photonics 1(6):489–495
90. Wood AD, Stankovic JA (2004) A taxonomy for denial-of-service attacks in wireless sensor networks . Handproceedings of Sensor Netw Compact Wireless and Wired Sensing Syst 8:739–763
91. Yang K, Forte D, Tehranipoor M (2015) Protecting endpoint devices in iot supply chain. In: 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp 351–356. IEEE
92. Yang K, Forte D, Tehranipoor M (2016) Ucr: An unclonable chipless rfid tag. In: 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp 7–12. IEEE
93. Yang K, Forte D, Tehranipoor M (2017) Cdta: A comprehensive solution for counterfeit detection, traceability, and authentication in the iot supply chain. ACM Trans Des Autom Electron Syst 22(3):42
94. Yang Z, Yue Y, Yang Y, Peng Y, Wang X, Liu W (2011) Study and application on the architecture and key technologies for iot. In: 2011 International Conference on Multimedia Technology (ICMT), pp 747–751. IEEE
95. Yinon J (2003) Peer reviewed: detection of explosives by electronic noses
96. Zeller M, Scheer G (2009) Add trip security to arc-flash detection for safety and reliability. In: Power Systems Conference, 2009. PSC'09., pp 1–8. IEEE
97. Zhang ZK, Cho MCY, Shieh S (2015) Emerging security threats and countermeasures in iot. In: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp 1–6. ACM